

What is claimed is:

1. A combinational circuit comprising:

5 a plurality of multipliers, independently performing two or more multiplications for coded digital signals in a Galois extension field  $GF(2^m)$ , where  $m$  is an integer equal to or greater than 2,

wherein said multipliers include

10 an input side XOR calculator,

an AND calculator, and

an output side XOR calculator, and

wherein said multipliers share said input side XOR calculator.

15 2. The combinational circuit according to claim 1, wherein the input of said multipliers is commonly used.

3. The combinational circuit according to claim 1, that is  
20 used for:

an error location calculator that calculates an error location for a digital signal transmitted using wavelength division multiplexing, and

for an error value calculator.

25 4. The combinational circuit according to claim 1, wherein syndromes obtained by said coded digital signal are input.

5. The combinational circuit according to claim 1, that is

used for at least one of decoding, error correction and encryption.

6. The combinational circuit according to claim 1, that is  
5 used for a coding circuit and a decoding circuit for cryptography.

7. A combinational circuit for performing a logical sum  
calculation for a Galois extension field  $GF(2^m)$ , where m is  
10 an integer equal to or greater than 2, comprising:

a plurality of multipliers, each of which includes an  
adder connected between an AND calculator and an output side  
XOR calculator,

wherein said output side XOR calculator is used in  
15 common, and

wherein outputs of said AND calculators in said  
multipliers are added by said adders, and addition results  
are calculated by said output side XOR calculator that is  
used in common.

8. The combinational circuit according to claim 7, wherein  
said multipliers have an input that is commonly used, and  
said input side XOR calculator is used in common by said  
multipliers.

9. The combinational circuit according to claim 7, that is  
used for:

an error location calculator for calculating an error  
location for a digital signal transmitted using wavelength

division multiplexing, and  
an error value calculator.

10. The combinational circuit according to claim 7, wherein  
5 syndromes obtained by said coded digital signal are input.

11. The combinational circuit according to claim 7, that is  
used for at least one of decoding, error correction and  
encryption.

10 12. The combinational circuit according to claim 7 that is  
used for a coding circuit and a decoding circuit for  
cryptography.

15 13. An encoder including the combinational circuit  
according to claim 1 or claim 7.

14. A decoder including the combinational circuit according  
to claim 1 or claim 7.

20 15. A semiconductor device used for processing a digital  
signal, said device comprising:

input means, for receiving a coded digital signal;

25 processing means, for processing said coded digital  
signal and for calculating coefficients of error locator  
polynomial and coefficients of error value polynomial; and

output means, for outputting a digital signal obtained  
by correcting errors using said coefficients of error  
locator polynomial and said coefficients of error value

polynomial,

wherein said input means is constituted by a sequential circuit, and said processing means is constituted by a combinational circuit.

5

16. The semiconductor device according to claim 15, wherein said combinational circuit includes:

a plurality of multipliers, independently performing two or more multiplications for coded digital signals in a Galois extension field  $GF(2^m)$ , where m is an integer equal to or greater than 2,

10

wherein said multipliers include

an input side XOR calculator,

an AND calculator, and

15

an output side XOR calculator, and

wherein said multipliers share said input side XOR calculator.

17. The semiconductor device according to claim 15, wherein said combinational circuit includes:

20

a logical sum calculator for a Galois extension field  $GF(2^m)$ , where m is an integer equal to or greater than 2,

wherein said multipliers include an adder connected between said AND calculator and said output side XOR calculator,

25

wherein said output side XOR calculator is used in common, and

wherein outputs of said AND calculators in said multipliers are added by said adders, and addition results

are calculated by said output side XOR calculator that is used in common.

18. The semiconductor device according to claim 15, wherein  
5 said multipliers have commonly used input, and said input side XOR calculator is used in common by said multipliers.

19. The semiconductor device according to claim 15, wherein  
10 said combinational circuit is used for an error location calculator, for calculating an error location for a digital signal transmitted using wavelength division multiplexing, and for an error value calculator.

20. The semiconductor device according to claim 15 that is  
15 used for at least one of decoding, error correction and encryption.